AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An integrated secure videoconferencing communications system, comprising:

an inverse multiplexer for receiving and converting data;

a black side switch having a first relay that includes a first contact, a second contact, and a third contact, and coupled to the inverse multiplexer via the third contact;

an encryption device coupled to the second contact of the black side switch;

a red side switch having a second relay that includes a first contact, a second contact, and a third contact, and coupled to the encryption device via the second contact;

a codec coupled to the red side switch via the third contact of the red side switch; and

a controller coupled to the black side and the red side switches for powering down the switches in a secure mode and powering up the switches in a non-secure mode, wherein in the secure mode the relays default to connect the encryption device into a communication path ~~controlling connection paths of the first contacts and second contacts of the black side and the red side switches~~.

2. (Original) The system of claim 1, wherein if the system is operating in a secure mode, the controller disables the first contacts of the black side and the red side switches, and the second contacts of the black side and red side switches are enabled to connect data path via the encryption device.

3. (Original) The system of claim 1, wherein if the system is operating in a non-secure mode, the controller enables the first contacts of the black and the red side switches.

4. (Original) The system of claim 1, further comprising means for on-screen dialing.

5. (Original) The system of claim 1, further comprising fiber optic isolation between all secure and non-secure signals.

6. (Original) The system of claim 1, wherein the system is in a secure operating mode when power is not supplied to the system.

7. (Original) The system of claim 1, further including:

a first fiber optics modem coupled to the first contact of the black side switch; and

a second fiber optics modem coupled to the first contact of the red side switch,

wherein data is communicated between the inverse multiplexer and the codec via the first and the second fiber optics modems.

8. (Original) The system of claim 1, further including a dial isolator module coupled to the codec by a first interface, the dial isolator further coupled to the inverse multiplexer by a second interface.

9. (Original) The system of claim 1, wherein the black side switch is coupled to the inverse multiplexer via an RS-530/449 interface.

10. (Original) The system of claim 1, wherein the red side switch is coupled to the codec via an RS-530/449 interface.

11. (Original) The system of claim 1, further including a power control module coupled to the controller and the first and the second fiber optics modems.

12. (Original) The system of claim 11, wherein the power control module terminates power supplied to the first and the second fiber optics modems when the system is operating in a secure mode.

13. (Original) The system of claim 1, further including a status indicator coupled to the controller for indicating an operating mode.

14. (Original) The system of claim 1, further including a switch coupled to the controller

for selecting an operating mode.

15. (Original) The system of claim 1, wherein the encryption device is coupled to the black side and the red side switches via an RS-530/449 interface.

16. (Original) The system of claim 1, wherein the codec includes a serial interfaced videoconferencing codec.

17. (Original) The system of claim 1, wherein the encryption device includes KIV 7 module.

18. (Original) The system of claim 1, wherein the encryption device includes KIV 19 module.

19. (Currently Amended) A method for providing secure communications, comprising:

determining an operating mode;

if the operating mode is secure mode, powering down and defaulting to ~~enabling~~ second contacts of two switches and communicating data between the two switches via a secure module; and

if the operating mode is non-secure mode, powering up and enabling first contacts of the two switches and communicating data between the two switches directly.

20. (Original) The method of claim 19, further including displaying the operating mode.

21. (Original) The method of claim 19, further including if the operating mode is non-secure mode, routing data between the two switches via a plurality of fiber optics modems.

22. (Original) The method of claim 19, further including if the operating mode is secure, routing data between the two switches through encryption devices and disconnecting the non-secure path between the two switches.

23. (Original) The method of claim 19, further including if the operating mode is secure, terminating power from a plurality of fiber optics modems coupling the two switches.

24. (Original) The method of claim 19, further including converting ISDN channel data to high speed RS-530/499 data.

25. (Currently Amended) An integrated secure videoconferencing communications system, comprising:

an inverse multiplexer for receiving and converting data;

a black side switch connected to the inverse ~~invert~~ multiplexer;

an encryption device connected to the black side switch;

a red side switch connected to the encryption device, and connected to the black side switch;

a codec connected to the red side switch; and

a controller for controlling the black side and the red side switches to power down and default to ~~enable either~~ a secure path connection between the black side and the red side switches via the encryption device or to power up and enable a non secure path connection directly between the black side and the red side switches.